DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Security Requirements Guides (SRGs)
and
Security Technical Implementation Guides (STIGs)

Sue Kreigline

16 May 2019

DISA Cyber Standards Branch

Agenda

- What is a SRG?
- What is a STIG?
- Who are the “STIG” people?
- What is our authority?
- How is a STIG Developed?
- What is the “Sunset” list?
- What STIG automation is available?
- What is the SRG/STIG Maintenance Process?
- Where is the SRG/STIG content?
- Questions

What is a SRG?

- **Security Requirements Guide (SRG)**
- **Collections of requirements applicable to a given technology family, a product category, or an organization in general**
- **Non-product specific requirements to mitigate sources of security vulnerabilities consistently and commonly encountered across information technology (IT) systems and applications**
- **Can be used if no specific STIG is available for a technology**

What is a STIG?

- **Security Technical Implementation Guide (STIG)**
- **Operationally implementable compendium of DoD IA controls, security regulations, and best practices for securing an IA or IA-enabled device (operating system, network, application software, etc.)**
- **Security guidance for such actions as mitigating insider threats, containing applications, preventing lateral movements, and securing information system credentials**

Who are the STIG People?

- **Defense Information Systems Agency**
  - Risk Management Executive
    - Standards & Analysis Division
      - Cyber Standards Branch – RE11
- **Mission:**
  - Develop and disseminate operationally implementable secure configuration guidance for use throughout the DoD
- **We are not the:**
  - DoD approver for the procurement or use of a product or technology
  - National Information Assurance Partnership (NIAP)
  - National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)
  - DoD Unified Capabilities (UC) Approved Products List (APL)

What is our Authority?

Based on DoDI 8500.01, “Cybersecurity”, dated 14 March 2014

"2. DIRECTOR, DISA. Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 13 of this enclosure, the Director, DISA:

b. Develops and maintains Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code risk categories and usage guides.”

How is a STIG Developed?

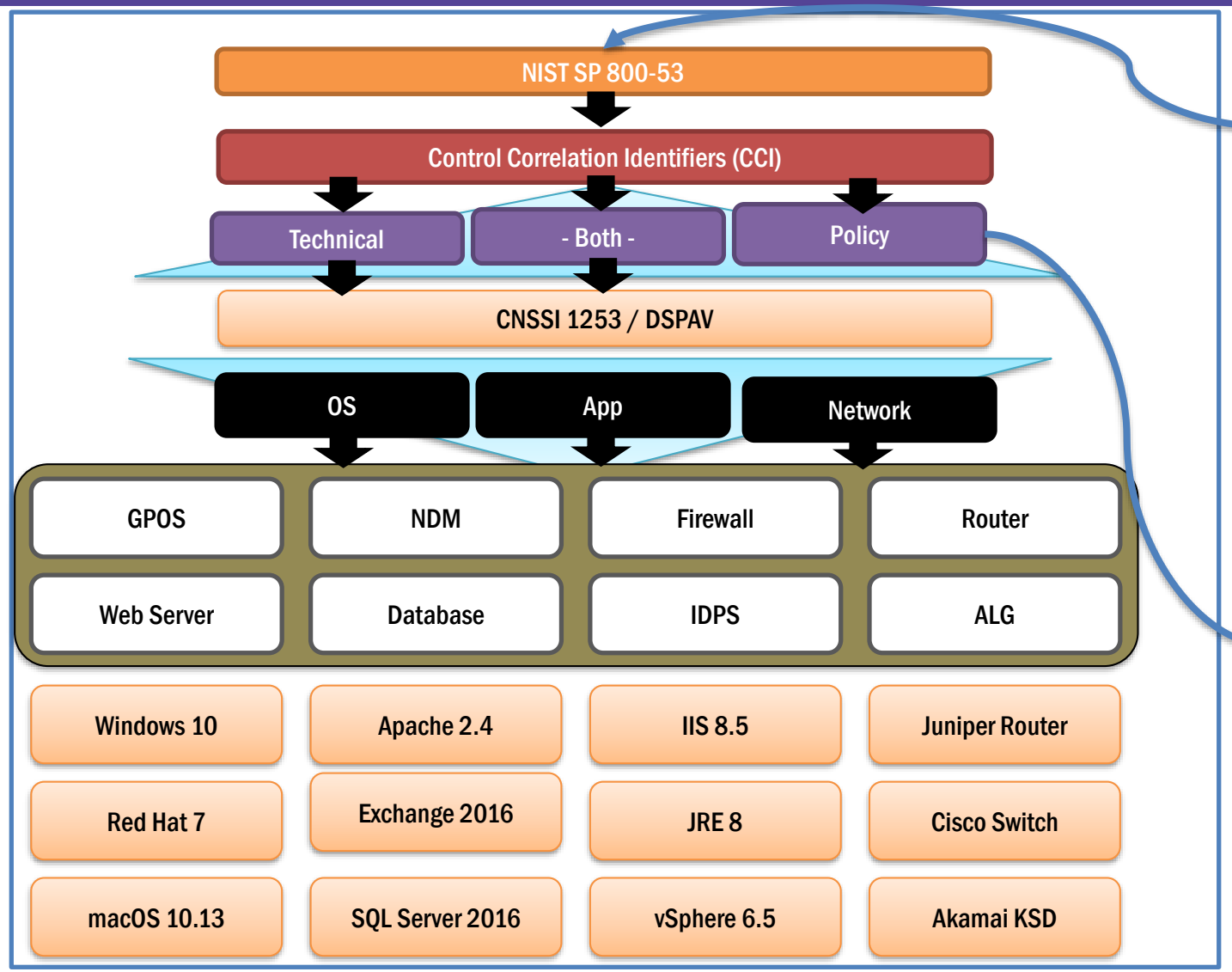
Cybersecurity Controls

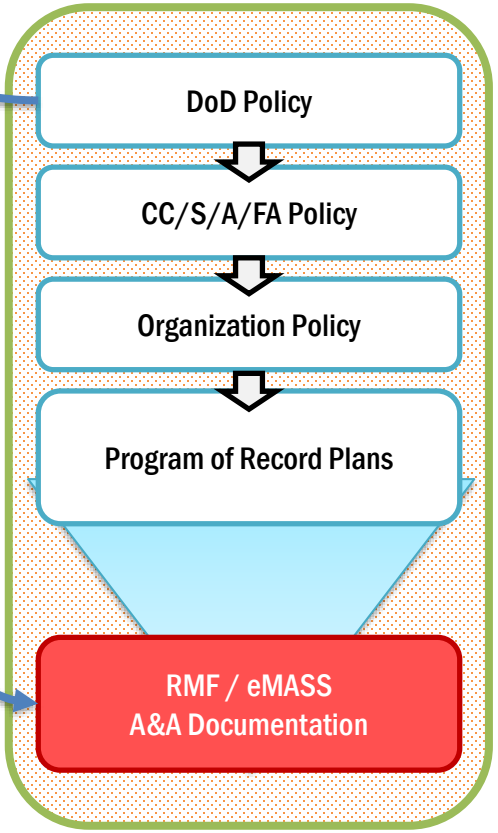
Breakdown Into Actionable Events (CCIs)

DoD Baseline Selection

SRGs

STIGs





What is the “Sunset” List?

- **List of documents no longer maintained**
- **Reasons documents are moved to “Sunset”**
  - Vendor no longer supports product
    - CAT I added for “no support”
  - Newer Version STIG has been released
  - Document no longer viable
- **Documents should be used as long as products being used**

What STIG Automation is Available?

- **DISA Produced Benchmarks**
  - Adobe Acrobat Reader DC
  - Google Chrome for Windows
  - Microsoft .NET Framework 4
  - Microsoft Internet Explorer 11
  - Microsoft Windows 10
  - Microsoft Windows Server (2008, 2012, 2016)
  - Microsoft Windows Defender A/V
  - Microsoft Windows Firewall
  - Red Hat 6
  - Red Hat Enterprise Linux 7
  - Solaris (10, 11)
- **Benchmarks produced using Security Content Automation Protocol (SCAP)**
- **Benchmarks work in HBSS, ACAS and SCC**

What is the SRG/STIG Maintenance Process?

- **Process**
  - Examine open tickets
  - Determine scope of work for each ticket
  - Determine if “fix” can be included in this release
  - “Fix” included in release
- **Quarterly Releases**
  - January
  - April
  - July
  - October
- **Ad hoc Releases**
  - “Fix” is too important to wait for quarterly release

Help Desk Email: DISA.STIG_spt@mail.mil

Where is the SRG/STIG Content?

http://iase.disa.mil/stigs

- **More than 350 security guides**
- **Manual and Automated (SCAP) Content**
- **STIG Viewer**
  - Enables off-line data entry
  - Provide capability to view one or multiple STIGs in human-readable format
- **STIG Applicability Tool**
  - Assists in determining what SRG/STIGs apply to a specific situation
- **Windows 10 Secure Host Baseline Download**

Questions

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**

visit us

DISA Booth 1929

follow us

Facebook/USDISA

Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at **www.disa.mil/about/industry-partners**.